UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,252	02/17/2004	Pratyush Moghe	TIZOR-001	9651

50086 7590 05/11/2009

LAW OFFICE OF DAVID H. JUDSON
15950 DALLAS PARKWAY
SUITE 225
DALLAS, TX 75248

EXAMINER	
JUNG, DAVID YIUK	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
05/11/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mail@davidjudson.com

Office Action Summary	Application No.	Applicant(s)	
	10/780,252	MOGHE, PRATYUSH	
	Examiner	Art Unit	
	David Y. Jung	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *11/28/2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-29 and 40-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-29 and 40-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-29, 40-51 are presented.

Response to Arguments

Applicant's arguments filed have been fully considered but they are not persuasive.

As noted in a previous Office Action, the allowable subject matter concerned content-level monitoring and trending of a network comprising mining of the packet database. Yet, the presented claims no longer have any of these features. Furthermore, all claims in the record are now significantly broader than claim 25 of the original filing. That claim was noted as clearly anticipated by admissions over the prior art.

"Changing over time" was explicitly noted in a previous Office Action as to be novel if this "changing over time" was not historical. In the context of the new claims 1-29, 40-51, this phrase "changing over time" is used in such a way that would refer to historical data. As noted by Applicant in the specification, the prior art already had packet analysis, real-time functioning, and changing content. Indeed, as Applicant noted, there is an entire body of knowledge regarding these matters. See, for instance, the entire bibliography of books and articles that Applicant has cited in the specification. In particular, the newly presented claims are precisely directed to the pieces of prior art that is discussed in page 6 of the revised specification.

As noted in a previous Office Action, the allowable subject matter was already noted. The cancelled limitations, such as the limitations cancelled from claim 1, are the allowable subject matter.

CLAIM REJECTIONS

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:
A person Shall be entitled to a patent unless -
(a) theinvention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-29, 40-51 are rejected under 35 U.S.C. 102(a) as being clearly anticipated by admissions over the prior art.

The prior art, as discussed in the specification (and not merely discussed in the first few pages), refer to the previous types of analysis of anomalies. These anomalies, as noted by Applicant, already had packet analysis, real-time functioning, and changing content. Indeed, as Applicant noted, there is an entire body of knowledge regarding these matters. See, for instance, the entire bibliography of books and articles that Applicant has cited in the specification.

Some of the claims (claims 1-29, 40-51 generally) recite packet analysis. This alone is not sufficient because the prior art (as admitted by Applicant) does acquire data from packets. See page 6 of the specification. Some of the claims (claims 1-29, 40-51 generally) recite real- time functioning. This alone is not sufficient because the prior art does some (albeit not all of the functions as in claim 1) functions in real-time. See, for

instance, the discussion regarding intrusion detection, such as from Escamilla, Lippman, LaPadula, etc. that are noted in the specification. Note the Intrusion detection work in real-time.

Claim 1: A method of performing an application layer semantic analysis to detect information access anomalies (the first paragraph, page 6 of the specification of this application which directly mentions such analysis to be "classical.")
, comprising: a) capturing data packets on the network; b) filtering the captured data packets to detect information content; c) processing packets based on semantics of of an application or protocol; d) generating a quantitative representation; (the second paragraph, page 6 of the specification of this application which directly mentions such statistical techniques to be "classical")
e) deriving a content signature from the quantitative representation; f) deriving a prototypical model of that includes a frequency view of a set of content signatures accessed by a given user, where the set of content signatures are indicative of content that is changing over time; and g) detecting an information access anomaly by detecting a given deviation from the prototypical model (the third paragraph, page 6 of the specification of this application which directly mentions such use of historical data to be "classical.")
Claims 2-29, 41-48: these features, as discussed in the previous Office Actions, were already noted by Applicant to be prior art. See page 6 of the specification.

49. A computer-implemented method of detecting an information access anomaly, comprising: monitoring data packets indicative of changing content over time; generating a prototypical model; and performing a semantic analysis against the prototypical model to identify an application level information access anomaly(the third paragraph, page 6 of the specification of this application which directly mentions such use of historical data to be "classical.").

50. A computer program product comprising a computer-readable storage medium encoded with processor-executable program instructions for implementing the method of claim 49.

This was already noted as prior art. The specification already mentions a computer - which would necessarily have these features.

51. Apparatus including a processor and a computer-readable storage medium, the computer-readable storage medium encoded with processor-executable program instructions for implementing the method of claim 49.

This was already noted as prior art. The specification already mentions a computer - which would necessarily have these features.

Conclusion

1. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

The art made of record and not relied upon is considered pertinent to applicant's disclosure. The art disclosed general background.

Points of Contact

Any response to this action should be mailed to:

Commissioner for Patents

Alexandria, VA 22313.

or faxed to:

(571) 273-8300, (for formal communications intended for entry)

Or:

(571) 273-3836 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Jung whose telephone number is (571) 272-3836 or Kambiz Zand whose telephone number is (571) 272-3811.

/David Y Jung/

Acting Examiner of Art Unit 2434

David Jung

David Jung

Patent Examiner